

## ARITHMETIC ACTIONS ON CYCLOTOMIC FUNCTION FIELDS

A. KONTOGEORGIS AND K. WARD

ABSTRACT. We derive the group structure for cyclotomic function fields obtained by applying the Carlitz action for extensions of an initial constant field. The tame and wild structures are isolated to describe the Galois action on differentials. We show that the associated invariant rings are not polynomial.

## 1. INTRODUCTION

Let  $\mathbb{F}_q$  denote the finite field of  $q$  elements, where  $q = p^r$  is a power of the prime integer  $p$ . Let  $d$  be a nonnegative integer. Consider the rational function field  $\mathbb{F}_{q^d}(T)$ . The Carlitz exponential map for  $\mathbb{F}_{q^d}$  is defined as

$$\tau_{q^d}(u) = Tu + u^{q^d}, \quad u \in \overline{\mathbb{F}_q(T)}.$$

This defines an action by  $T$ , which may be extended  $\mathbb{F}_{q^d}$ -linearly to an action by elements of  $\mathbb{F}_{q^d}[T]$ , according to

$$(1) \quad M = \sum a_i T^i \in \mathbb{F}_{q^d}[T], \quad u_{q^d}^M = \sum a_i \tau_{q^d}^i(u).$$

The Carlitz modules  $\Lambda_{q^d, M}$  are then the torsion  $\mathbb{F}_{q^d}$ -modules within the algebraic closure  $\overline{\mathbb{F}_{q^d}(T)}$  via this action. We note that this does depend upon the choice of  $d$ . Henceforth, for a polynomial  $M \in \mathbb{F}_{q^d}[T]$ , we let  $K_{q^d, M}$  denote the *cyclotomic function field* for  $\mathbb{F}_{q^d}$  and  $M$ , which is obtained by adjoining to  $\mathbb{F}_{q^d}(T)$  the Carlitz module  $\Lambda_{q^d, M}$ . These function fields are called *cyclotomic* as they are derived from an exponential function in positive characteristic and enjoy many of the same properties of the classical cyclotomic extensions of  $\mathbb{Q}$  [12, Chapter 12].

We suppose henceforth that  $M \in \mathbb{F}_q[T]$  and that  $M$  splits over  $\mathbb{F}_{q^d}[T]$ . As in [14], one may determine explicitly the holomorphic differentials for  $K_{q^d, M}$ . Here, we relate this situation to the original cyclotomic function field  $K_{q, M}$ . We first prove the essential result:

**Theorem 1.1.**  $K_{q, M} \subset K_{q^d, M}$ .

This allows us to understand the differentials of  $K_{q, M}$  in terms of those of  $K_{q^d, M}$  by examining Galois covers. Henceforth, we denote

$$H_{q^d, M} := \text{Gal}(K_{q^d, M} / \mathbb{F}_{q^d} K_{q, M}).$$

One then obtains naturally the following tower of fields:

$$\begin{array}{ccc}
 & & K_{q^d, M} \\
 & \nearrow^{H_{q^d, M}} & \downarrow \\
 \mathbb{F}_{q^d} K_{q, M} & & \mathbb{F}_{q^d}(T) \\
 \downarrow & \searrow & \downarrow \\
 K_{q, M} & & \mathbb{F}_q(T)
 \end{array}$$

The group  $H_{q^d, M}$  was studied by Chapman [3] when  $M \in \mathbb{F}_q[T]$  is square-free, in order to give a normal integral basis of the ring of integers of  $K_{q, M}$  over  $\mathbb{F}_q[T]$ . This cannot be done in the same fashion if  $M$  contains a square  $P^2$  of an irreducible polynomial  $P \in \mathbb{F}_q[T]$ , as under the wild ramification at  $P$  in  $K_{q, M}$  the integer ring is no longer a free  $\mathbb{F}_q[T]$  module. Here, we study  $H_{q^d, M}$  more generally, as the genus is invariant under constant extensions, so that identification of the space of differentials of  $K_{q, M}$  reduces to identifying those differentials of  $K_{q^d, M}$  which are fixed by the action of  $H_{q^d, M}$ .

The Frobenius map on  $\mathbb{F}_{q^d}/\mathbb{F}_q$  permutes the roots of  $M$ , and the group  $H_{q^d, M}$  is nontrivial: Even in the case where  $M = P$  is irreducible over  $\mathbb{F}_q[T]$  and  $\deg(M) = d$ ,  $|H_{q^d, M}| = (q^d - 1)^{d-1}$ . The group  $H_{q^d, M}$  may be described in a simple, explicit way in terms of the Carlitz action. The abelian Galois group  $\text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T))$  is naturally a  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -module, and denoting  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma \rangle$ , the group  $H_{q^d, M}$  may be described as

$$H_{q^d, M} = (\sigma - 1)\text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T)).$$

This is proven in Lemma 2.3. In general, the absolute Galois group  $\hat{\mathbb{Z}} = \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$  acts on the cyclotomic function fields, and this action may be precisely described using the group structure of  $H_{q^d, M}$ . This point of view, where the *arithmetic* part of a Galois group is acting on the *geometric* part, is a unifying notion. One may see, for example, the seminal article of Y. Ihara [7].

We devote Section 2 to the description of  $H_{q^d, M}$ . In Section 3, we examine the tame structures arising within this group and give an explicit Kummer generator of the tame part of  $H_{q^d, M}$ . Section 4 describes the wild component of  $H_{q^d, M}$ , including the higher ramification groups and different. Cyclotomic function fields may also be viewed as towers of Kummer and Artin-Schreier extensions, whose form we give in Section 5. Section 6 describes the Galois module structure of the differentials of  $K_{q, M}$ . We concern ourselves with the group  $H_{q^d, M}$  as its invariants yield differentials on the constant extension  $\mathbb{F}_{q^d} K_{q, M}$  of  $K_{q, M}$ , and constant extensions do not alter the genus, so that it suffices to give a description of the differentials of  $\mathbb{F}_{q^d} K_{q, M}$  in order to understand the Galois module structures for  $K_{q, M}$ . The holomorphic differentials are comprised of products of generators of the Carlitz modules. In order to compute the  $H_{q^d, M}$ -invariant differentials, we will employ modular invariant theory. For fixed  $q^d$  and  $M$ , our constructions provide an algorithm for the computation of invariants and holomorphic differentials for the

function field  $K_{q,M}$ . As we show in Section 6, the invariant ring for the algebra of Carlitz generators is not polynomial. This shows that a closed formula for a basis for holomorphic differentials will be quite complicated in general, despite that it can be done when  $M$  splits over  $\mathbb{F}_q$  [14].

## 2. PRELIMINARY RESULTS

**2.1. Inclusions of cyclotomic function fields.** We now give the proof of Theorem 1.1.

*Proof of Theorem 1.1.* For a global field  $K$ , let  $S(L/K)$  denote the collection of places of  $K$  which split completely in  $L$ . By Bauer's theorem [12, Theorem 11.5.1], we have for a global function field  $K$  and two Galois extensions  $L_1$  and  $L_2$  of  $K$  that

$$L_2 \subset L_1 \Leftrightarrow S(L_1/K) \subset S(L_2/K).$$

Thus, the extension  $K_{q,M}$  is contained in  $K_{q^d,M}$  if, and only if, the places of  $\mathbb{F}_q(T)$  which split in  $K_{q^d,M}$  also split in  $K_{q,M}$ . For a place  $\mathfrak{p}$  of  $\mathbb{F}_q(T)$ , we let  $\mathfrak{P}$  denote a place of  $K_{q,M}$  above  $\mathfrak{p}$ ,  $\mathfrak{p}_{q^d}$  a place of  $\mathbb{F}_{q^d}(T)$  above  $\mathfrak{p}$ , and  $\mathfrak{P}_{q^d}$  a place of  $K_{q^d,M}$  above  $\mathfrak{p}$ . If  $\mathfrak{p}$  denotes a place of  $K = \mathbb{F}_q(T)$  which splits completely in  $K_{q^d,M}$ , then we have

$$[\mathfrak{O}_{\mathfrak{P}_{q^d}}/\mathfrak{P}_{q^d} : \mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}] = 1,$$

where  $\mathfrak{O}_{\mathfrak{P}_{q^d}}$  denotes the valuation ring for  $\mathfrak{P}_{q^d}$  in  $K_{q^d,M}$  and  $\mathfrak{P}_{q^d}$  its maximal ideal,  $\mathfrak{o}_{\mathfrak{p}}$  the valuation ring for  $\mathfrak{p}$  in  $K$  and  $\mathfrak{p}$  its maximal ideal. In the analogous notation, we thus have

$$[\mathfrak{O}_{\mathfrak{P}_{q^d}}/\mathfrak{P}_{q^d} : \mathfrak{o}_{\mathfrak{p}_{q^d}}/\mathfrak{p}_{q^d}][\mathfrak{o}_{\mathfrak{p}_{q^d}}/\mathfrak{p}_{q^d} : \mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}] = 1.$$

In particular, it follows that

$$[\mathfrak{O}_{\mathfrak{P}_{q^d}}/\mathfrak{P}_{q^d} : \mathfrak{o}_{\mathfrak{p}_{q^d}}/\mathfrak{p}_{q^d}] = 1,$$

and that the place  $\mathfrak{p}_{q^d}$  of  $\mathbb{F}_{q^d}(T)$  is completely split in  $K_{q^d,M}$ . Notice that  $\mathfrak{p}$  cannot be infinity, as infinity is not split in cyclotomic extensions (the ramification index is the size of the constant field minus one [12, Theorem 12.4.6]). It follows that the place  $\mathfrak{p}_{q^d}$  is associated with an irreducible polynomial  $P_{q^d} \in \mathbb{F}_{q^d}[T]$ . By cyclotomic function field theory, for example, Proposition 12.5.2 of Villa-Salvador [12], the inertia degree of  $\mathfrak{p}_{q^d}$  is equal to the order of  $P_{q^d}$  modulo  $M$ . In fact, we may write

$$P = \prod_{i=1}^k P_i$$

in  $\mathbb{F}_{q^d}[T]$ , where  $P$  is associated with  $\mathfrak{p}$  in  $\mathbb{F}_q[T]$  and the polynomials  $P_i$  are the (distinct) factors of  $P$  in  $\mathbb{F}_{q^d}(T)$ . We also know that the finite places of  $\mathbb{F}_{q^d}$  which divide  $M$  ramify in  $K_{q^d,M}$ , and hence are not completely split. Also, we know that  $P_{q^d} = P_i$  for some  $i$ , but also that  $P_{q^d}$  was an arbitrary choice of place, which could be done as the extensions we consider are all Galois. Thus  $(P_i, M) = 1$  for all  $i = 1, \dots, k$ , from which it follows that  $(P, M) = 1$ . By cyclotomic function field theory, we also know that the order of  $P$  modulo  $M$  in  $\mathbb{F}_q[T]$  is equal to the inertia degree of  $\mathfrak{p}$  in  $K_{q,M}$ . For each  $i = 1, \dots, k$ , let  $o_{h,i}$  denote the order of  $P_i$  modulo  $M$  in  $\mathbb{F}_{q^d}[T]$ . Thus

$$P_i^{o_{h,i}} \equiv 1 \pmod{M}, \quad i = 1, \dots, k.$$

We may then write  $P_i^{o_{h,i}} - 1 = FM$  for some  $F \in \mathbb{F}_{q^d}[T]$ . As the Galois action of  $\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)$  is transitive, it follows that for any  $j = 1, \dots, k$ , there exists  $\sigma \in \text{Gal}(\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T))$  such that  $\sigma(P_i) = P_j$ . It follows that

$$P_j^{o_{h,i}} - 1 = \sigma(P_i)^{o_{h,i}} - 1 = \sigma(P_i^{o_{h,i}}) - 1 = \sigma(P_i^{o_{h,i}} - 1) = \sigma(FM) = \sigma(F)M,$$

where  $\sigma(F) \in \mathbb{F}_{q^d}[T]$  by definition of the Galois action of  $\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)$ . It follows by symmetry that the order of each  $P_i$  modulo  $M$  is the same. We therefore set  $o_h := o_{h,i}$  for  $i = 1, \dots, k$ . It follows from this that

$$P^{o_h} = \left( \prod_{i=1}^k P_i \right)^{o_h} = \prod_{i=1}^k P_i^{o_h} \equiv \prod_{i=1}^k 1 = 1 \pmod{M},$$

and hence the order  $o_P$  of  $P$  modulo  $M$  is at most  $o_h$ . As the polynomials  $P_i$ ,  $i = 1, \dots, k$  are completely split in  $K_{q^d, M}$ , it follows from the cyclotomic theory that  $o_h = 1$ , and thus  $o_P \leq o_h = 1$ . Thus, the place  $\mathfrak{p}$  associated with  $P$  is completely split in  $K_{q, M}$ . We have thus shown that if a place  $\mathfrak{p}$  of  $K = \mathbb{F}_q(T)$  splits completely in  $K_{q^d, M}$ , then it must also split completely in  $K_{q, M}$ . Hence, by Bauer's theorem, it follows that  $K_{q, M} \subset K_{q^d, M}$ .  $\square$

Henceforth, as we frequently distinguish between  $\mathbb{F}_q[T]$  and  $\mathbb{F}_{q^d}[T]$ , we denote  $A_1 := \mathbb{F}_q[T]$  and  $A_d := \mathbb{F}_{q^d}[T]$ . The following properties of Galois extensions may be easily deduced from the previous theorem (see also [12, Chapter 12]).

- $\text{Gal}(\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)) \cong \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$
- $\text{Gal}(K_{q, M}/\mathbb{F}_q(T)) \cong (A_1/MA_1)^*$ .
- $\text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T)) \cong (A_d/MA_d)^*$ .
- $\text{Gal}(K_{q^d, M}/\mathbb{F}_q(T)) \cong (A_d/MA_d)^* \times \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ .

We now fix a basis  $1 = v_1, \dots, v_d$  of  $\mathbb{F}_{q^d}$  as a vector space over  $\mathbb{F}_q$ , and we write

$$A_d \cong A_1 \oplus v_2 A_1 \oplus \dots \oplus v_d A_1.$$

As  $M \in A_1$  by definition, we then have

$$A_d/MA_d \cong A_1/MA_1 \oplus v_2 A_1/MA_1 \oplus \dots \oplus v_d A_1/MA_1.$$

Also, the group  $\text{Gal}(K_{q^d, M}/K_{q, M})$  fits in the short exact sequence

$$1 \rightarrow \text{Gal}(K_{q^d, M}/K_{q, M}) \rightarrow (A_d/MA_d)^* \times \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \rightarrow (A_1/MA_1)^* \rightarrow 1.$$

For ease of notation, we define  $G_{q^d, M} := \text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T))$ . It is well-known that

$$(2) \quad G_{q^d, M} \cong (A_d/MA_d)^*,$$

where the Galois action is induced by the Carlitz action by elements of  $(\mathbb{F}_{q^d}[T]/M)^*$ . The Galois inclusion  $\mathbb{F}_q(T) \subset \mathbb{F}_{q^d}(T) \subset K_{q^d, M}$  gives rise to another short exact sequence:

$$\begin{array}{ccc} 1 \rightarrow \text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T)) & \longrightarrow & \text{Gal}(K_{q^d, M}/\mathbb{F}_q(T)) \xrightarrow{\pi} \text{Gal}(\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)) \rightarrow 1 \\ \parallel & & \parallel \\ G_{q^d, M} & & \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) \end{array}$$

By standard arguments of group theory, the Galois group  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  acts by conjugation on  $G_{q^d, M}$  of an inverse section of the map  $\pi$ . We note that as the group  $G_{q^d, M}$  is abelian, this action is well defined, i.e., independent of the choice of the section of  $\pi$ .

**2.2. The group  $G_{q^d, P}$  as a  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -module.** We identify each divisor  $D \in (A_d/MA_d)^*$  with the element  $\rho_D \in G_{q^d, M}$  under the isomorphism (2). The natural action of  $\sigma \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  on  $\rho_D$  is given by conjugation. As such, we have

$$\sigma \rho_D \sigma^{-1} = \rho_{\sigma(D)},$$

where  $\sigma(D)$  simply denotes the image of  $D \in A_d$  under the natural action of  $\sigma$  in  $\mathbb{F}_{q^d}$ . We have

$$\rho_D(u) := D *_d u = u^{q^s} + b_{s-1} u^{q^{s-1}} + \cdots + Du,$$

so that

$$\sigma \rho_D \sigma^{-1}(u) = u^{q^s} + \sigma(b_{s-1}) u^{q^{s-1}} + \cdots + \sigma(D)u,$$

where  $*_d$  denotes the Carlitz action over  $\mathbb{F}_{q^d}(T)$ . In what follows, we emphasise that  $G_{q, M} = \text{Gal}(K_{q, M}/\mathbb{F}_q(T))$  is isomorphic to  $\text{Gal}(\mathbb{F}_{q^d} K_{q, M}/\mathbb{F}_{q^d}(T))$ , as one may deduce from (??).

**Lemma 2.3.** *The group  $H_{q^d, M} = \text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d} K_{q, M})$  in the short exact sequence*

$$(3) \quad 1 \rightarrow H_{q^d, M} \rightarrow G_{q^d, M} \rightarrow G_{q, M} \rightarrow 1$$

*satisfies*

- (1)  $\sigma(H_{q^d, M}) = H_{q^d, M}$
- (2)  $H_{q^d, M} = (\sigma - 1)G_{q^d, M}$ .

*Proof.* (1) The natural action on subgroups of a Galois groups is the conjugation action. The field

$$\mathbb{F}_{q^d} K_{q, M} = K_{q^d, M}^{H_{q^d, M}}$$

is a subfield of  $K_{q^d, M}$  which is invariant, albeit not pointwise, under the action of  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ . Let  $\sigma$  be a generator of the cyclic group  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ . As both

$$\sigma(\mathbb{F}_{q^d} K_{q, M}) = K_{q^d, M}^{\sigma H_{q^d, M} \sigma^{-1}} \quad \text{and} \quad \sigma(\mathbb{F}_{q^d} K_{q, M}) = \mathbb{F}_{q^d} K_{q, M},$$

we have that  $\sigma H_{q^d, M} \sigma^{-1} = H_{q^d, M}$ .

- (2) We will prove first that  $(\sigma - 1)D \in H_{q^d, M}$  for each element  $D \in G_{q^d, M}$ . The group  $G_{q^d, M}$  consists of classes of invertible elements  $D \in \mathbb{F}_{q^d}[T]$  modulo  $M$ . Let  $\sigma \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  be a generator of the cyclic Galois group. As  $G_{q, M}$  is the Galois group of a geometric extension, it follows that the group  $G_{q, M} = G_{q^d, M}/H_{q^d, M}$  is pointwise  $\sigma$ -invariant. Thus  $\sigma(D)/D \in H_{q^d, M}$ .

Since the group  $G_{q^d, M}$  is abelian, the map

$$\begin{aligned} G_{q^d, M} &\xrightarrow{\Phi} G_{q^d, M} \\ \alpha &\longmapsto \sigma(\alpha)\alpha^{-1} \end{aligned}$$

is a group homomorphism. The kernel of  $\Phi$  consists of elements  $D \in G_{q^d, M} \cong (\mathbb{F}_{q^d}[T]/M)^*$  which are left invariant under the action of  $\sigma$ , hence it is isomorphic to  $G_{q, M}$ . On the other hand, we have proven that  $\text{Im}(\Phi) \subset H_{q^d, M}$ . Thus  $|\text{Im}(\Phi)| = |G_{q^d, M}|/|G_{q, M}|$ . Since by definition  $|G_{q, M}| = |G_{q^d, M}|/|H_{q^d, M}|$ , we obtain  $|\text{Im}(\Phi)| = |H_{q^d, M}|$ , and we arrive at

$$H_{q^d, M} = (\sigma - 1)G_{q^d, M},$$

concluding the proof. □

**Remark 2.4.** The group  $G_{q^d, M}$  is naturally a  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -module. The group  $G_{q, M}$  is the space of coinvariants

$$G_{q, M} = (G_{q^d, M})_{\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)} = \frac{G_{q^d, M}}{(\sigma - 1)G_{q^d, M}}.$$

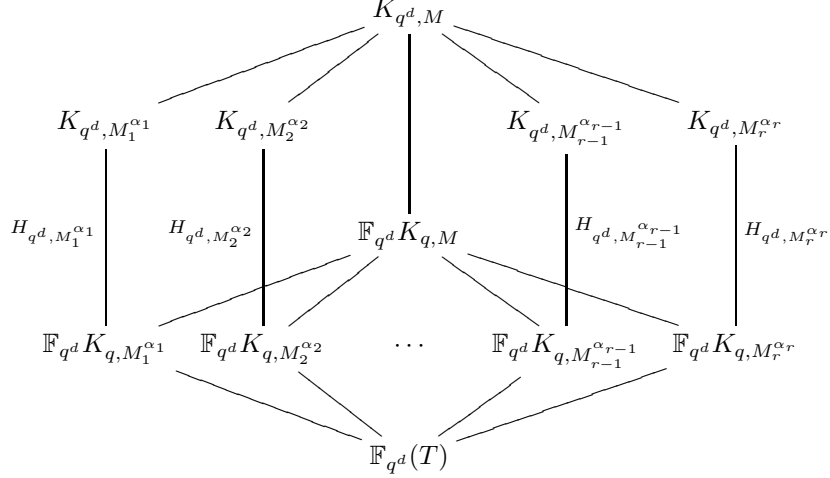
**2.5. Reduction to irreducible factors of  $M$ .** We now reduce the computation of the structure of the group  $H_{q^d, M}$  to the study of the corresponding groups for the irreducible components of  $M$ . Let  $M \in \mathbb{F}_q[T]$  be of degree  $k$ , with factorization in  $\mathbb{F}_q[T]$

$$M = \prod_{j=1}^r M_j^{\alpha_j},$$

where the polynomials  $M_j$  are irreducible, monic and of degree  $s_j | d$ . In the finite field  $\mathbb{F}_{q^d}$ , the polynomials  $M_j \in \mathbb{F}_q[T]$  factor into linear factors in  $\mathbb{F}_{q^d}[T]$ . We write

$$M = \prod_{j=1}^r \prod_{i=1}^{s_j} (T - \rho_{i,j})^{\alpha_j}, \quad \rho_{i,j} \in \mathbb{F}_{q^d}.$$

The field  $K_{q, M}$  is the compositum of the fields  $K_{q, M_j^{\alpha_j}}$ , each of which is, in turn, a subfield of  $K_{q^d, M_j^{\alpha_j}}$ . This yields the following diagram:



We have

$$\text{Gal}(K_{q^d, M}/\mathbb{F}_{q^d}(T)) \cong \times_{j=1}^r \text{Gal}(K_{q^d, M_j^{\alpha_j}}/\mathbb{F}_{q^d}(T))$$

and

$$H_{q^d, M} = \times_{j=1}^r H_{q^d, M_j^{\alpha_j}}.$$

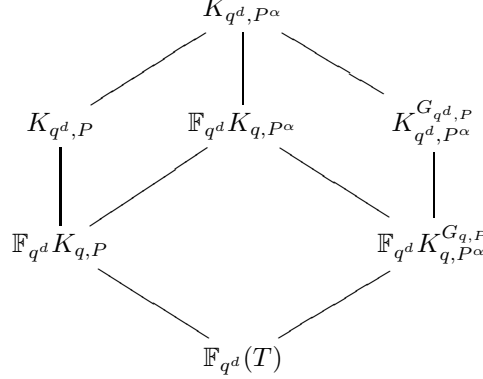
The problem of determining the structure of the group  $H_{q^d, M}$  may therefore be reduced to determination of each of the groups  $H_{q^d, M_i^{\alpha_i}}$ . This means that we may assume  $M$  to be a power  $P^\alpha$  of an irreducible polynomial  $P \in \mathbb{F}_q[T]$ . Thus, as a consequence of Lemma 2.3, we now study the group  $G_{q^d, P}$ , where  $P$  is an irreducible polynomial in  $\mathbb{F}_q[T]$  of degree  $s | d$ . The splitting field of  $P$  is equal to  $\mathbb{F}_{q^s}$ . By definition, we have the following short exact sequence:

$$(4) \quad 1 \rightarrow P_{q^d, P^\alpha} \rightarrow G_{q^d, P^\alpha} \rightarrow G_{q^d, P} \rightarrow 1,$$

where

$$P_{q^d, P^\alpha} = \{D \in \mathbb{F}_{q^d}[T] \mid D \equiv 1 \pmod{P}\}.$$

The field  $K_{q^d, P^\alpha}$  is the compositum of a generalised Artin-Schreier extension with the Kummer extension  $K_{q^d, P}/\mathbb{F}_{q^d}(T)$ . The subfield  $\mathbb{F}_{q^d}K_{q, P^\alpha}$  has a similar decomposition, into a generalised Artin-Schreier extension with Galois group  $\mathbb{Z}/q^{\alpha-1}\mathbb{Z}$  with the Kummer extension  $\mathbb{F}_{q^d}K_{q, P}/\mathbb{F}_{q^d}(T)$ . We have the following tower of fields:



**Lemma 2.6.** *Let  $\sigma \in \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ , and for each  $i = 1, \dots, \alpha$ , let*

$$F_i := K_{q, P^i}^{G_{q, P}}.$$

*Then for each  $i = 1, \dots, \alpha$ , the generator  $\sigma$  of the Galois group  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  satisfies*

- (1)  $\sigma(K_{q^d, P^i}) = K_{q^d, P^i}$ .
- (2)  $\sigma(F_i) = F_i$ .

*Proof.* By construction, we have  $\sigma(\mathbb{F}_{q^d}(T)) = \mathbb{F}_{q^d}(T)$  and  $\sigma(K_{q^d, P^i}) = K_{q^d, P^i}$ , for each  $i = 1, \dots, \alpha$ . The Galois group  $\text{Gal}(K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T))$  is congruent to the direct product of the cyclic group  $\mathbb{F}_{q^d}^*$  with the  $p$ -group  $\text{Gal}(F_\alpha/\mathbb{F}_{q^d}(T))$ . By definition, we have that  $\mathbb{F}_{q^d}(T) \subset \sigma(F_\alpha) \subset K_{q^d, P^\alpha}$ , whence  $\sigma(F_\alpha)$  corresponds to a Galois group  $H$  which is isomorphic to a cyclic group of order  $q^d - 1$ . As there is a unique such subgroup in  $\text{Gal}(K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T))$ , it follows that  $\sigma(F_\alpha) = F_\alpha$ .

The result for  $F_i$  for each  $i = 1, \dots, \alpha - 1$  follows by induction.  $\square$

We note that property (2) in Lemma 2.6 implies that  $(\sigma - 1)G_{q^d, P}$  corresponds to a subgroup of  $H_{q^d, P}$ , and by order comparisons, we obtain that the unique such submodule of  $G_{q^d, P}$  is given by the image of the map  $\sigma - 1$ . For a realisation of a Kummer model of  $K_{q, P}$ , we refer to Section 3.

### 3. TAME STRUCTURE

In order to understand  $H_{q^d, P}$ , we will describe the character group of  $G_{q^d, P}$  using the torsion of the Carlitz module. We know by prime decomposition [12, Chapter 12] that

$$(5) \quad \Lambda_{q^d, P} = \bigoplus_{i=1}^s \Lambda_{q^d, T - \rho_i}.$$

The torsion modules  $\Lambda_{q^d, T - \rho_i}$  are defined as

$$\Lambda_{q^d, T - \rho_i} := \{z \in \overline{\mathbb{F}_q(T)} : z^{q^d} + (T - \rho_i)z = 0\}.$$

Let  $\lambda_i$  be a generator of  $\Lambda_{q^d, T-\rho_i}$  as an  $A_d$ -module. Then  $\lambda_i$  satisfies the equation

$$(6) \quad \lambda_i^{q^d-1} = -(T - \rho_i).$$

**Lemma 3.1.** *Let  $\sigma$  be a generator of the cyclic group  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ . Then*

$$\sigma(\lambda_i) = \begin{cases} \zeta_{\sigma, i} \lambda_{i+1} & \text{if } 1 \leq i < s \\ \zeta_{\sigma, d} \lambda_1 & \text{if } i = s, \end{cases}$$

where  $\zeta_{\sigma, i}$  is a  $(q^d - 1)$ st root of unity, which depends on both  $\sigma$  and  $i$ .

*Proof.* Consider the action of  $\sigma$  on (6). If  $i < s$ , then

$$(\sigma \lambda_i)^{q^d-1} = -\sigma(T - \rho_i) = -(T - \sigma(\rho_i)) = -(T - \rho_{i+1}) = \lambda_{i+1}^{q^d-1}.$$

The result follows in this case. The proof for  $i = s$  is the same, except that  $\sigma(\rho_s) = \rho_1$ .  $\square$

On the other hand, the action of  $G_{q^d, P}$  on  $\lambda_i$  is given by multiplication by elements in  $\mathbb{F}_{q^d}^*$ . Indeed, if  $f \in \mathbb{F}_{q^d}[T]$  and  $(f, P) = 1$ , then  $f(\rho_i) \neq 0$  for all  $i = 1, \dots, s$ . By definition of the Carlitz action  $*_d$ , and the fact that  $\lambda_i$  is a  $(T - \rho_i)$ -torsion point it follows that

$$(7) \quad \sigma_f \lambda_i = f *_d \lambda_i = f(\rho_i) \cdot \lambda_i.$$

We note that  $f(\rho_i) \in \mathbb{F}_{q^d}$ , whence  $f(\rho_i)^{q^d-1} = 1$ .

**Definition.** Let  $\zeta$  be a fixed choice of primitive  $(q^d - 1)$ st root of unity. We define the dual elements  $\{\sigma_k^*\} \in G_{q^d, P}^*$  such that

$$\sigma_k^*(\sigma_\ell) = \begin{cases} 1 & \text{if } k \neq \ell \\ \zeta & \text{if } k = \ell. \end{cases}$$

**Remark 3.2.** As  $s \mid d$  we have that  $(q^s - 1) \mid (q^d - 1)$ . The element

$$\zeta_1 := \zeta^{\frac{q^d-1}{q^s-1}}$$

generates a cyclic subgroup of  $G_{q^d, P}$  of order  $q^s - 1$ .

**Lemma 3.3.** *For each  $i_0 = 1, \dots, s$ , consider the polynomials*

$$f_{i_0}(x) := \left( 1 - \prod_{\substack{i=1 \\ i \neq i_0}}^s (x - \rho_i) \right) = 1 - \frac{P(x)}{x - \rho_{i_0}} \in \mathbb{F}_{q^d}[x].$$

*Then*

$$\sigma_{f_{i_0}} *_d \lambda_j = \left( 1 - \prod_{\substack{i=1 \\ i \neq i_0}}^s (\rho_j - \rho_i) \right) \cdot \lambda_j.$$

*Proof.* The proof follows immediately from (7).  $\square$

**Lemma 3.4.** *For each  $i_0 = 1, \dots, s$ , consider the elements*

$$Z_{i_0} := \left( 1 - \prod_{\substack{i=1 \\ i \neq i_0}}^s (\rho_{i_0} - \rho_i) \right).$$



Then

$$Z_{i_0} = Z_1^{q^{i_0-1}}.$$

Furthermore, the elements  $Z_{i_0}$  are primitive  $(q^s - 1)$ st roots of unity.

*Proof.* The number of generators of a cyclic group of order  $q^s - 1$  is equal to  $\phi(q^s - 1)$ , where  $\phi$  denotes the Euler totient function. Furthermore, it is well-known that  $s \mid \phi(q^s - 1)$ . We find, recall that  $\rho_1 = \zeta_1$  and  $\rho_i = \zeta_1^{q^{i-1}}$  for  $1 \leq i \leq s - 1$ ,

$$\begin{aligned} Z_{i_0} &= \left( 1 - \prod_{\substack{i=1 \\ i \neq i_0}}^s (\zeta_1^{q^{i_0-1}} - \zeta_1^{q^{i-1}}) \right) \\ &= \left( 1 - \prod_{i=2}^s (\zeta_1^{q^{i_0-1}} - \zeta_1^{q^{i+i_0-2}}) \right) \\ &= \left( 1 - \prod_{i=2}^s (\zeta_1 - \zeta_1^{q^{i-1}}) \right)^{q^{i_0-1}} = Z_1^{q^{i_0-1}}, \end{aligned}$$

which concludes the proof.  $\square$

Recall that each generator  $\lambda_i$  of  $\Lambda_{q^d, T-\rho_i}$  satisfies (6). The elements  $\lambda_i$  define characters  $\sigma_{\lambda_i}^* = \chi_{\lambda_i}$  by Kummer theory, which are given by

$$\sigma_{\lambda_i}^*(\sigma) = \lambda_i^\sigma \lambda_i^{-1},$$

for each  $\sigma \in G_{q^d, P}$ . In particular, we find that

$$\sigma_{\lambda_i}^*(\sigma_{f_j}) = \lambda_i^{\sigma_{f_j}} \lambda_i^{-1} = \begin{cases} Z_1^{q^{j-1}} & \text{if } i = j \\ 1 & \text{if } i \neq j. \end{cases}$$

We now write  $Z_1 = \zeta_1^\alpha$  for some  $\alpha \in \mathbb{N}$ ,  $(\alpha, q^s - 1) = 1$ . The character group of  $G_{q^d, P}$  is non-canonically isomorphic to  $G_{q^d, P}$ . Moreover, letting  $n = q^s - 1$ , the quotient map in (3) gives

$$G_{q^d, P} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 1,$$

which by duality yields the injection of the cyclic group  $\mathbb{Z}/n\mathbb{Z}$

$$1 \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow G_{q^d, P}^*.$$

For each  $i = 1, \dots, s$ , let  $\sigma_i$  be chosen generators of the  $i$ th direct summand in the decomposition given in (5) of the group  $G_{q^d, P}$ , and consider a dual basis  $\sigma_i^*$  of  $G_{q^d, P}^*$  such that

$$\sigma_i^* \sigma_j = \delta_{ij} \rho_1 = \delta_{ij} \zeta_1,$$

where  $\delta_{ij}$  is Kronecker's  $\delta$ . An injection

$$\iota : \langle g \rangle = \mathbb{Z}/n\mathbb{Z} \rightarrow G_{q^d, P}^*$$

is described by giving the coordinates of the generator  $g$ , i.e.,

$$(8) \quad \iota(g) = \prod_{i=1}^s (\sigma_i^*)^{\frac{q^d-1}{q^s-1} b_i}.$$

Furthermore, the element  $\iota(g)$  has order  $n$  if, and only if, at least one of the integers  $b_i$  is prime to  $n$ . Also, the character  $\iota(g)$  given in (8) is associated (via the Kummer correspondence) to the element

$$(9) \quad L = \prod_{i=1}^s \lambda_i^{\frac{q^d-1}{q^s-1} b_i}, \text{ which satisfies } L^{q^s-1} = (-1)^s \prod_{i=1}^s (T - \rho_i)^{b_i}.$$

**Lemma 3.5.** *For each  $i = 1, \dots, s$ , the exponent  $b_i$  in (9) may be explicitly and recursively determined.*

*Proof.* For the Frobenius generator  $\sigma$  of the cyclic group  $\text{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$  and  $L$  as defined in (9), the element  $\sigma(L)$  is a generating radicand of the Kummer extension, and therefore has the form

$$\sigma(L) = L^\mu a^{q^s-1},$$

for some  $\mu \in \mathbb{N}$  such that  $(\mu, q^s - 1) = 1$  and some  $a \in \mathbb{F}_{q^d}(T)$ . This implies that

$$\lambda_1^{b_s} \prod_{i=2}^s \lambda_i^{b_{i-1}} = \prod_{i=1}^s \lambda_i^{b_i \mu} a^{q^s-1},$$

which in turn implies for each  $i = 2, \dots, s$  that

$$b_{i-1} = \mu b_i \pmod{q^s - 1}$$

and also that

$$b_s = \mu b_1 \pmod{q^s - 1}.$$

We let  $\mu'$  be the inverse of  $\mu$  modulo  $q^d - 1$ . This yields

$$(10) \quad \begin{aligned} b_1 \mu' &\equiv b_2 \pmod{q^s - 1} \\ b_2 \mu' &\equiv b_3 \pmod{q^s - 1} \\ &\dots\dots\dots \\ b_{s-1} \mu' &\equiv b_s \pmod{q^s - 1} \\ b_s \mu' &\equiv b_1 \pmod{q^s - 1}. \end{aligned}$$

Therefore,  $b_i = (\mu')^{i-1} b_1$  for each  $i = 2, \dots, s$ . As  $b_s = (\mu')^{s-1} b_1$  (10) implies that

$$(\mu')^s \equiv 1 \pmod{q^s - 1}.$$

We can thus select  $\mu' = q$  to obtain the appropriate value of  $\mu' \pmod{q^s - 1}$ . It may also be assumed without loss that  $b_1 = 1$ .  $\square$

We have thus proven the following result.

**Proposition 3.6.** *The model of the function field  $\mathbb{F}_{q^d} K_{q,P}$  is given by the Kummer extension:*

$$(11) \quad L^{q^s-1} = (-1)^s \prod_{i=1}^s \left( T - \zeta_1^{q^{i-1}} \right)^{q^i}.$$

The Galois module structure of such extensions is known by the work of Boseck. Also, by Kummer theory, the ramification index of the factors of the generating radicands is given by

$$e_i = \frac{q^s - 1}{(q^s - 1, b_i)}.$$

Furthermore, by the theory of Carlitz modules, we may also easily see that there is ramification over all places corresponding to the linear factors  $T - \rho_i$  of  $P$  in  $A_d$ . It

follows that  $(b_i, q^s - 1) = 1$ , for each  $i = 1, \dots, s$ . As there is ramification of degree  $q - 1$  at infinity in  $K_{q,P}/\mathbb{F}_q(T)$ , we obtain

$$\sum_{\nu=1}^s b_i = 1 + q + \dots + q^{s-1}.$$

We have the following tower of fields and ramified places over  $\mathbb{F}_{q^d}(T)$ :

$$\begin{array}{ccccccc} K_{q^d,M} & B_{1,1} \cdots B_{1,q^s-1} & \cdots & B_{s,1} \cdots B_{s,q^s-1} & Q_1, \dots, Q_t \\ \downarrow & \downarrow \frac{q^d-1}{q^s-1} & & \downarrow \frac{q^d-1}{q^s-1} & \downarrow \frac{q^d-1}{q-1} \\ \mathbb{F}_{q^d} K_{q,M} & B_1 & \cdots & B_s & B_{\infty,1}, \dots, B_{\infty, \frac{q^s-1}{q-1}} \\ \downarrow \mathbb{F}_{q^s}^* & \downarrow q^s-1 & & \downarrow q^s-1 & \downarrow q-1 \\ \mathbb{F}_{q^d}(T) & P_1 & \cdots & P_s & P_{\infty} \end{array}$$

**Remark 3.7.** In the special case  $s = d$ , there is no ramification over  $B_1, \dots, B_s$  in the extension  $K_{q^d,P}/\mathbb{F}_{q^d} K_{q,P}$ .

#### 4. WILD STRUCTURE

We now proceed to the case  $M = P^\alpha$ , where  $P \in \mathbb{F}_q[T]$  is again an irreducible polynomial of degree  $s \mid d$ . By previous arguments, it is easily seen that the abelian Galois group  $\text{Gal}(K_{q^d,P^\alpha}/\mathbb{F}_q(T))$  may be written as the direct product

$$\text{Gal}(K_{q^d,P^\alpha}/\mathbb{F}_q(T)) \cong G_{q^d,P} \times P_{q^d,P^\alpha}.$$

There is a very precise way to describe the group  $P_{q^d,P^\alpha}$ , which is also used in the elementary proof of the Kronecker-Weber theorem for rational function fields [10].

**Proposition 4.1** (Proposition 5.1 [10]). *Let  $r$  be a positive integer. The group  $P_{q^r,P^\alpha}$  is an abelian  $p$ -group. Let  $v_{q^r,n}(\alpha)$  denote the number of cyclic groups of order  $p^n$  in the decomposition of  $P_{q^r,P^\alpha}$ , where  $s = \deg P$ . Then*

$$v_{q^r,n}(\alpha) = \frac{q^{rs(\alpha - \lceil \frac{\alpha}{p^n} \rceil)} - q^{rs(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)} = \frac{q^{rs(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)} (q^{rs(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1)}{p^{n-1}(p-1)},$$

where  $\lceil x \rceil$  denotes the ceiling function on  $\mathbb{Q}$ , i.e., the minimum integer greater than or equal to  $x$ .

In particular, Proposition 4.1 holds for both  $P_{q,P^\alpha}$  and  $P_{q^d,P^\alpha}$  by setting  $r = 1$  and  $r = d$ , respectively. For the Kummer extensions  $P_{q,P}$  and  $P_{q^d,P}$ , we must realise the Galois group

$$H'_{q^d,P^\alpha} := \text{Gal} \left( K_{q^d,P^\alpha}^{G_{q^d,P}} / \mathbb{F}_{q^d} K_{q,P^\alpha}^{G_{q,P}} \right).$$

For this, we obtain the exact sequence

$$0 \rightarrow H'_{q^d,P^\alpha} \rightarrow \text{Gal}(K_{q^d,P^\alpha}^{G_{q^d,P}} / \mathbb{F}_{q^d}(T)) \rightarrow \text{Gal}(\mathbb{F}_{q^d} K_{q,P^\alpha}^{G_{q,P}} / \mathbb{F}_{q^d}(T)) \rightarrow 0,$$

where the structure of the abelian  $p$ -group

$$P_{q,P^\alpha} = \text{Gal}(\mathbb{F}_{q^d} K_{q,P^\alpha}^{G_{q,P}} / \mathbb{F}_{q^d}(T))$$

is given by Proposition 4.1.

**Corollary 4.2.**  $H'_{q^d, P^\alpha} = (\sigma - 1)P_{q^d, P^\alpha}$ .

*Proof.* This follows in the same manner as Lemma 2.3, as  $\sigma(H'_{q^d, P^\alpha}) = H'_{q^d, P^\alpha}$  and  $(\sigma - 1)D \in H'_{q^d, P^\alpha}$  for every  $D \in P_{q^d, P^\alpha}$ .  $\square$

In the extension  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d}K_{q, P^\alpha}$ , there is generally wild ramification: According to [12, Proposition 12.4.5], the place at infinity is ramified in the extension  $\mathbb{F}_{q^d}K_{q, P^\alpha}$  with index  $q - 1$  and in the extension  $K_{q^d, P^\alpha}$  with ramification index  $q^d - 1$ . Moreover, the ramification degree of  $P$  in the extension  $\mathbb{F}_{q^d}K_{q, P^\alpha}/\mathbb{F}_{q^d}(T)$  is equal to  $q^{s\alpha} - q^{s(\alpha-1)}$ , while the ramification degree of  $P$  in extension  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)$  is given by  $q^{d\alpha} - q^{d(\alpha-1)}$  [12, Proposition 12.3.14], whence the ramification in extension  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d}K_{q, P^\alpha}$  is given by

$$e = \frac{q^{d\alpha} - q^{d(\alpha-1)}}{q^{s\alpha} - q^{s(\alpha-1)}} = q^{(d-s)(\alpha-1)} \frac{q^d - 1}{q^s - 1}.$$

We thus obtain the following diagram, where  $s = (q^{d\alpha} - q^{d(\alpha-1)})/(q - 1)$ :

$$\begin{array}{ccccc} K_{q^d, P^\alpha} & P' & \infty_{1,1}, \dots, \infty_{1,q-1} & & \infty_{s,1}, \dots, \infty_{s,q-1} \\ \downarrow H & \downarrow e & \downarrow \frac{q^d-1}{q-1} & & \downarrow \frac{q^d-1}{q-1} \\ \mathbb{F}_{q^d}K_{q, P^\alpha} & P_1 & \infty_1 & \dots & \infty_s \\ \downarrow & \downarrow & \swarrow q-1 & & \searrow q-1 \\ \mathbb{F}_{q^d}(T) & P & & \infty & \end{array}$$

The irreducible polynomial  $P$  factors in  $\mathbb{F}_{q^d}$  as

$$(12) \quad P(T) = \prod_{i=1}^s (T - \zeta_1^{q^{i-1}}),$$

where  $\zeta_1$  is a primitive  $(q^s - 1)$ st root of 1. We denote  $P_i = T - \zeta_1^{q^{i-1}}$  ( $i = 1, \dots, s$ ).

**Lemma 4.3.** *The quotient  $A_d/P^\alpha$  is  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -equivariantly isomorphic to the direct sum of vector spaces:*

$$A_d/P^\alpha = \bigoplus_{i=1}^{\alpha} A_1/P.$$

*The group of units  $(A_d/P^\alpha)^*$  satisfies*

$$(A_d/P^\alpha)^* = (A_d/P)^* \oplus \left( \bigoplus_{i=2}^{\alpha} A_d/P \right).$$

*Proof.* It is clear that the following sequence is exact:

$$(13) \quad 0 \rightarrow P^{\alpha-1}/P^\alpha \rightarrow A_1/P^\alpha \rightarrow A_1/P^{\alpha-1} \rightarrow 1.$$

Therefore, we can prove by induction that

$$(A_d/P^\alpha) = A_d/P \oplus P/P^2 \oplus P^2/P^3 \oplus \dots \oplus P^{\alpha-1}/P^\alpha.$$

On the other hand, the map

$$\begin{aligned} A_d/P &\rightarrow P^i/P^{i+1} \\ f \bmod P &\mapsto f \cdot P^i \bmod P^{i+1} \end{aligned}$$

is a  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -equivariant isomorphism, since  $P^i$  is a  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -invariant element.  $\square$

Let  $f \in A_d/P^\alpha$ . Consider the class  $f_0$  of  $f$  modulo  $P^{\alpha-1}$ , i.e.,

$$f \bmod P^\alpha \equiv f_0 + P^{\alpha-1}f_1 \bmod P^\alpha, \quad f \bmod P^{\alpha-1} \equiv f_0 \bmod P^{\alpha-1}.$$

We consider now the multiplication

$$\begin{aligned} f \cdot g &\equiv (f_0 + P^{\alpha-1}f_1)(g_0 + P^{\alpha-1}g_1) \\ &\equiv f_0g_0 + (\bar{f}_0g_1 + f_1\bar{g}_0)P^{\alpha-1} \bmod P^\alpha, \end{aligned}$$

where  $\bar{f}_0, \bar{g}_0$  denote the classes of  $f_0, g_0 \bmod P$ . It is clear by induction that  $f$  is invertible if, and only if,  $\bar{f}_0 \equiv f \bmod P$  is invertible. We define the following filtration:

$$(14) \quad N_t := \{D \bmod P^\alpha : D \equiv 1 \bmod P^t\}.$$

The group  $N_1$  is the wild part of  $(A_d/P^\alpha)^*$ . We have the following short exact sequence

$$1 \rightarrow N_{t+1} \rightarrow N_t \rightarrow P^t/P^{t+1} \rightarrow 1,$$

where the group structure on  $N_t$  is multiplicative while the structure on  $P^t/P^{t+1}$  is additive. The wild part of  $H_{q^d, P^\alpha}$  consists of elements of the form  $\sigma(D)D^{-1}$  in  $N_1$ , where  $D \in N_1$ . The filtration of  $N_1$

$$N_1 \supset N_2 \supset \dots N_i \supset \dots$$

induces a filtration on  $H_{q^d, P^\alpha}$ :

$$H^1 = H_{q^d, P^\alpha} \cap N_1 \supset H^2 = H_{q^d, P^\alpha} \cap N^2 \supset \dots \supset H^i = H_{q^d, P^\alpha} \cap N_i \supset \dots$$

We observe that

$$\frac{H^i}{H^{i+1}} = \{\sigma(D)D^{-1} \bmod H^{i+1} : D \in H^i\},$$

and the latter group can be identified with the image of the operator  $(\sigma - 1)(f)$  in the additive group  $P^i/P^{i+1} \cong A_d/P$ .

**Lemma 4.4.** *The space  $A_d/P \cong \bigoplus_{i=1}^s \mathbb{F}_{q^d}$ . An element  $f \in A_d/P$  is mapped to the coordinates  $(f(\zeta), f(\zeta^q), \dots, f(\zeta^{q^{s-1}})) \in \bigoplus_{i=1}^s \mathbb{F}_{q^d}$ . The action of the operator  $\sigma - 1$  on the coordinates  $(x_1, \dots, x_s) \in \bigoplus_{i=1}^s \mathbb{F}_{q^d}$  is given by:*

$$(x_1, \dots, x_s) \xrightarrow{\sigma-1} (x_s^q - x_1, x_1^q - x_2, \dots, x_{s-1}^q - x_s).$$

The kernel of  $\sigma - 1$  consists of elements  $(x_1, \dots, x_s)$  such that

$$x_1 \in \mathbb{F}_{q^d} : x_i = x_1^{q^{i-1}}, \quad i = 2, \dots, s.$$

Clearly this set has  $q^d$  elements since all elements are determined by the value of  $x_1$ . Therefore, the image of  $\sigma - 1$  has exactly  $q^{d(s-1)}$  elements.

**Remark 4.5.** Given an  $H_{q^d, P^\alpha}$ -module  $\mathcal{M}$ , the space of invariants  $\mathcal{M}^H$  is given by

$$\mathcal{M}^{H_{q^d, P^\alpha}} = \left( \left( \mathcal{M}^{H_{q^d, P^\alpha}^\alpha} \right)^{H_{q^d, P^\alpha}^{\alpha-1}/H_{q^d, P^\alpha}^\alpha} \dots \right)^{H_{q^d, P^\alpha}^1/H_{q^d, P^\alpha}^2}.$$

Since  $H^\alpha = H^\alpha/H^{\alpha+1}$ , we can apply recursively the computation of Lemma 4.4 in order to compute  $H_{q^d, P^\alpha}$ -invariants.

We now turn to ramification groups and the computation of the different. For each  $i \in \mathbb{Z}$  with  $i \geq -1$ , the  $i$ th ramification group of  $\mathfrak{P}|\mathfrak{p}$  is defined as

$$G_i(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G_{q^d, P^\alpha} \mid v_{\mathfrak{P}}(\sigma(x) - x) \geq i + 1 \text{ for all } x \in \mathfrak{D}_{\mathfrak{P}}\},$$

where  $\mathfrak{D}_{\mathfrak{P}}$  denotes the valuation ring at  $\mathfrak{P}$ . We denote  $G_i = G_i(\mathfrak{P}|\mathfrak{p})$ .

**Proposition 4.6.** (1) The groups  $N_k$  defined in (14) have order  $q^{ds(\alpha-k)}$  for  $1 \leq k \leq n$  and correspond to the upper ramification filtration at  $\mathfrak{P}|\mathfrak{p}$ .  
 (2) We have

- $G_0 = G_{q^d, P^\alpha}$ ,
- $G_i = N_k$  for all  $q^{d(k-1)} \leq i \leq q^{dk} - 1$  and  $1 \leq k \leq \alpha - 1$ , and
- $G_i = N_\alpha = \text{Id}$  for all  $i \geq q^{d(\alpha-1)}$ .

*Proof.* (1) [8, Prop. 2.2].

(2) This follows by the relation between upper and lower ramification filtrations [13, IV. sec. 3]. □

By Proposition 4.6, the lower ramification filtration is given by

$$\begin{aligned} G_0 &> G_1 = \cdots = G_{q^d-1} = N_1 \\ &> G_{q^d} = \cdots = G_{q^{2d}-1} = N_2 \\ &> G_{q^{2ds}} = \cdots = G_{q^{3d}-1} = N_3 \\ &> \quad \quad \quad \cdots \\ &> G_{q^{d(\alpha-2)}} = \cdots = G_{q^{d(\alpha-1)}} = N_{\alpha-1} \\ &> \{1\}. \end{aligned}$$

The ramification filtration for the group  $H_{q^d, P^\alpha}$  may be found by intersecting  $H_{q^d, P^\alpha}$  with  $G_i$ , so that

$$H_i := G_i \cap H_{q^d, P^\alpha}, \quad |H_i| = \begin{cases} (q^d - 1)^{s-1} q^{d(s-1)(\alpha-1)} & \text{if } i = 0 \\ q^{d(s-1)(\alpha-i)} & \text{if } i \geq 1. \end{cases}$$

We now determine the different  $\mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}$  of  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}$ .

**Proposition 4.7.**

$$\mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}} = \prod_{i=1}^s \prod_{\mathfrak{P}|\wp_i} \mathfrak{P}^A \prod_{\mathfrak{P}|\mathfrak{p}_\infty} \mathfrak{P}^B,$$

where with  $d = sl$ ,  $x$

$$\begin{aligned} (15) \quad A &= (\alpha q^{d\alpha} - (\alpha + 1)q^{d(\alpha-1)}) - (\alpha q^{s\alpha} - (\alpha + 1)q^{s(\alpha-1)}) \frac{q^{d\alpha} - q^{d(\alpha-1)}}{q^{\alpha s} - q^{(\alpha-1)s}} \\ &= \frac{q^{d(\alpha-1)}(q^d - q^s)}{q^s - 1}, \end{aligned}$$

and

$$(16) \quad B = (q^d - 2) - (q - 2) \frac{q^d - 1}{q - 1} = q \left( \frac{q^{d-1} - 1}{q - 1} \right).$$

*Proof.* As the extension  $K_{q^d, P}/\mathbb{F}_q(T)$  is separable, we may employ [12, Theorem 5.7.15]: Among separable extensions  $K \subset L \subset M$  of global fields, we have the functorial identity

$$(17) \quad \mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \text{con}_{L/M}(\mathfrak{D}_{L/K}).$$

We consider the two towers

$$\mathbb{F}_q(T) \subset K_{q, P^\alpha} \subset \mathbb{F}_{q^d} K_{q, P^\alpha} \subset K_{q^d, P^\alpha} \quad \text{and} \quad \mathbb{F}_q(T) \subset \mathbb{F}_{q^d}(T) \subset K_{q^d, P^\alpha}.$$

We may now proceed with computations within each of these towers.

- (1)  $\mathbb{F}_q(T) \subset K_{q, P^\alpha}$ . The different  $\mathfrak{D}_{K_{q, P^\alpha}/\mathbb{F}_q(T)}$  is given by [12, prop. 12.7.1]

$$\mathfrak{D}_{K_{q, P^\alpha}/\mathbb{F}_q(T)} = \mathfrak{P}^{\alpha q^{s\alpha} - (\alpha+1)q^{s(\alpha-1)}} \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{q-2},$$

where  $\mathfrak{P}$  is the unique place of  $K_{q, P^\alpha}$  above the place  $\mathfrak{p}$  of  $\mathbb{F}_q(T)$  associated with  $P$ .

- (2)  $\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q, P^\alpha}$  is unramified at all places of  $K_{q, P^\alpha}$ , whence

$$\mathfrak{D}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q, P^\alpha}} = (1).$$

- (3)  $\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)$  is also unramified at all places of  $\mathbb{F}_q(T)$ , whence

$$\mathfrak{D}_{\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)} = (1).$$

- (4) For the extension  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)$ : As  $s|d$  and the polynomial  $P$  thus splits completely in  $\mathbb{F}_{q^d}[T]$ , we denote each linear factor of  $P$  in  $\mathbb{F}_{q^d}[T]$  by  $\wp_i$ , so that  $P = \prod_{i=1}^s \wp_i$ . We obtain [12, Thm. 12.7.2]

$$\mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)} = \left[ \prod_{i=1}^s \prod_{\mathfrak{P}|\wp_i} \mathfrak{P} \right]^{\alpha q^{d\alpha} - (\alpha+1)q^{d(\alpha-1)}} \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{q^d-2}.$$

By (17), we may therefore write  $\mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}$  as

$$\begin{aligned} \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}^{-1} &= \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_q(T)}^{-1} \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/\mathbb{F}_q(T)}(\mathfrak{D}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/\mathbb{F}_q(T)}) \\ &= \left( \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)} \text{con}_{\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)}(\mathfrak{D}_{\mathbb{F}_{q^d}(T)/\mathbb{F}_q(T)}) \right)^{-1} \\ &\quad \times \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\mathfrak{D}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/\mathbb{F}_q(T)}) \\ &= \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)}^{-1} \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\mathfrak{D}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/\mathbb{F}_q(T)}) \\ &= \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)}^{-1} \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\mathfrak{D}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q, P^\alpha}} \\ &\quad \times \text{con}_{K_{q, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}(\mathfrak{D}_{K_{q, P^\alpha}/\mathbb{F}_q(T)})) \\ &= \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)}^{-1} \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\text{con}_{K_{q, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}(\mathfrak{D}_{K_{q, P^\alpha}/\mathbb{F}_q(T)})) \\ &= \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d}(T)}^{-1} \text{con}_{K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\mathfrak{D}_{K_{q, P^\alpha}/\mathbb{F}_q(T)}) \\ &= \left[ \prod_{i=1}^s \prod_{\mathfrak{P}|\wp_i} \mathfrak{P} \right]^{-(\alpha q^{d\alpha} - (\alpha+1)q^{d(\alpha-1)})} \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{-(q^d-2)} \\ &\quad \times \text{con}_{K_{q, P^\alpha}/K_{q^d, P^\alpha}} \left( \mathfrak{P}^{\alpha q^{s\alpha} - (\alpha+1)q^{s(\alpha-1)}} \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{q-2} \right) \end{aligned}$$

$$\begin{aligned}
&= \left[ \prod_{i=1}^s \prod_{\mathfrak{P}|\wp_i} \mathfrak{P} \right]^{-(\alpha q^{d\alpha} - (\alpha+1)q^{d(\alpha-1)})} \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{-(q^d-2)} \\
&\quad \times \left[ \prod_{i=1}^s \prod_{\mathfrak{P}|\wp_i} \mathfrak{P}^{\alpha q^{s\alpha} - (\alpha+1)q^{s(\alpha-1)}} \right]^{\frac{q^{d\alpha} - q^{d(\alpha-1)}}{q^{\alpha s} - q^{(\alpha-1)s}}} \left[ \prod_{\mathfrak{B}|\mathfrak{p}_\infty} \mathfrak{B}^{q-2} \right]^{\frac{q^d-1}{q-1}}.
\end{aligned}$$

The result follows.  $\square$

## 5. TOWER STRUCTURES

We now examine cyclotomic function fields as composites of towers of Kummer and Artin-Schreier extensions. Let  $P \in \mathbb{F}_q[T]$  be irreducible, whence  $P$  possesses only simple roots. We assume once more that  $\deg P = s \mid d$ . We now give the recursive definition for the cyclotomic function field  $K_{q^d, (T-\rho)^\alpha}$ .

**Lemma 5.1.** *Let  $(T-\rho) \in A_d$  be a factor of  $P$ , where  $\rho \in \mathbb{F}_{q^s} \cong A_1/P$ . Then the field  $K_{q^d, (T-\rho)^\alpha}$  may be described recursively by a tower of composita of explicitly determined Kummer and Artin-Schreier extensions over  $\mathbb{F}_{q^d}(T)$ .*

*Proof.* We first consider the case  $\alpha = 2$ , i.e., the cyclotomic function field  $K_{q^d, (T-\rho)^2}$  generated over  $\mathbb{F}_{q^d}(T)$  by the torsion points of  $(T-\rho)^2$ . By definition of the Carlitz action  $*_d$ , we have

$$\begin{aligned}
(T-\rho) *_d u &= u^{q^d} + (T-\rho)u \\
(T-\rho)^2 *_d u &= u^{q^{2d}} + \left( (T-\rho)^{q^d} + (T-\rho) \right) u^{q^d} + (T-\rho)^2 u.
\end{aligned}$$

We denote  $X = (T-\rho) *_d u$ . The equation

$$(T-\rho) *_d X = X^{q^d} + (T-\rho)X = 0$$

implies that either  $X = 0$  or  $X^{q^d-1} = -(T-\rho)$ . Let  $\lambda$  be a solution of the second equation, so that  $\lambda^{q^d-1} = -(T-\rho)$ . The general torsion point for  $(T-\rho)^2$  over  $\mathbb{F}_{q^d}$  may then be described by the equation

$$u^{q^d} + (T-\rho)u = \lambda.$$

We set  $u = U\lambda$ , which yields

$$U^{q^d} \lambda^{q^d} - \lambda^{q^d-1} \lambda U = \lambda,$$

whence we obtain

$$(18) \quad U^{q^d} - U = -\frac{1}{T-\rho}.$$



We have thus constructed the following tower of fields:

$$\begin{array}{ccc}
 & K_{q^d, (T-\rho)^2} & \\
 \swarrow & & \searrow \\
 \frac{\mathbb{F}_{q^d}(T)[U]}{\langle U^{q^d} - U = -\frac{1}{T-\rho} \rangle} & & \frac{\mathbb{F}_{q^d}(T)[\lambda]}{\langle \lambda^{q^d-1} = -(T-\rho) \rangle} \\
 \searrow & & \swarrow \\
 & \mathbb{F}_{q^d}(T) &
 \end{array}$$

The field  $K_{q^d, (T-\rho)^2}$  is therefore the compositum of a Kummer extension and an Artin-Schreier extension, where a root  $u$  of the torsion point equation  $(T-\rho)^2 *_d u$  is given by  $u = U\lambda$ . One may now easily proceed inductively: Let  $U_2 := U$  be the element given in (18), and let  $u_2 = U_2\lambda$ . A solution of  $(T-\rho)^3 *_d u_3 = 0$  is then given by

$$u_3^{q^d} + (T-\rho)u_3 = u_2.$$

We set  $U_3 = u_3/\lambda$ . This yields  $U_3^{q^d} \lambda^{q^d} - \lambda^{q^d-1} \lambda U_3 = u_2$ , which in turn implies that

$$U_3^{q^d} - U_3 = -\frac{U_2}{T-\rho}.$$

(We note that  $u_2/\lambda^{q^d-1} = U_2$ .) In this way, we may build a tower of successive Artin-Schreier extensions. We have thus obtained the extended diagram

$$(19) \quad
 \begin{array}{ccc}
 & K_{q^d, (T-\rho)^\alpha} & \\
 & \vdots & \swarrow \\
 & K_{q^d, (T-\rho)^3} & \frac{\mathbb{F}_{q^d}(T)[U_\alpha]}{\langle U_\alpha^{q^d} - U_\alpha = -\frac{U_{\alpha-1}}{T-\rho} \rangle} \\
 & \vdots & \vdots \\
 & K_{q^d, (T-\rho)^2} & \frac{\mathbb{F}_{q^d}(T)[U_3]}{\langle U_3^{q^d} - U_3 = -\frac{U_2}{T-\rho} \rangle} \\
 & \vdots & \vdots \\
 \mathbb{F}_{q^d}(T)(\lambda) & \xlongequal{\quad} K_{q^d, (T-\rho)} & \frac{\mathbb{F}_{q^d}(T)[U_2]}{\langle U_2^{q^d} - U_2 = -\frac{1}{T-\rho} \rangle} \\
 & \text{Kummer} & \\
 & \mathbb{F}_{q^d}(T) &
 \end{array}$$

This completes the proof.  $\square$

Within the diagram (19), we have described the Kummer model of the extension  $\mathbb{F}_{q^d} K_{q, P^\alpha} / \mathbb{F}_{q^d}(T)$ . By the arguments of §2 on Kummer covers, it thus remains to

describe the Artin-Schreier-Witt model of the extension

$$K_{q^d, P^\alpha}^{\mathbb{F}_q^*} / \mathbb{F}_{q^d}(T).$$

We may therefore prove the following corollary.

**Corollary 5.2.** *Let  $P \in \mathbb{F}_q[T]$  be irreducible of degree  $s \mid d$ . Then the field  $K_{q^d, P^\alpha}^{\mathbb{F}_q^*}$  may be described recursively by a tower of composita of explicitly determined Artin-Schreier extensions over  $\mathbb{F}_{q^d}(T)$ .*

*Proof.* For each linear factor  $T - \rho_i$  of  $P$ , we consider the generating elements  $U_j^{(i)}$ ,  $j = 1, \dots, \alpha$ , of the fields  $K_{q^d, (T - \rho_i)^\alpha}$ , each of which satisfies the equation

$$\left(U_j^{(i)}\right)^P - U_j^{(i)} = U_{j-1}^{(i)}.$$

By the Chinese remainder theorem once more, we obtain an equality with the compositum

$$K_{q^d, P^\alpha}^{\mathbb{F}_q^*} = \prod_{i=1}^s K_{q^d, (T - \rho_i)^\alpha}^{\mathbb{F}_q^*}.$$

As before, let  $\sigma$  be a generator of the cyclic group  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  such that  $\sigma(\rho_i) = \rho_{i+1}$ , for each  $i = 1, \dots, s-1$ , and  $\sigma(\rho_s) = \rho_1$ . For each  $i = 1, \dots, s-1$ , we have

$$\sigma(U_2^{(i)}) = U_2^{(i+1)} - a_i, \quad a_i \in \mathbb{F}_{q^d}.$$

We may normalise without loss the selection of elements  $U_2^{(i)}$  so that

$$\sigma(U_2^{(i)}) = U_2^{(i+1)}.$$

Proceeding inductively, we thus obtain

$$\sigma(U_j^{(i)}) = U_j^{(i+1)} \quad j = 2, \dots, \alpha.$$

By the correspondence of Artin-Schreier extensions to additive characters, we know that the field  $\mathbb{F}_{q^d} K_{q, P^2}^{\mathbb{F}_q^*}$  is given by an Artin-Schreier equation

$$y^{q^d} - y = \sum_{i=1}^s \frac{b_i}{U_1^{(i)}}, \quad U_1^{(i)} = T - \rho_i.$$

On the other hand, the field  $K_{q, P^2}$  is invariant under the action of the generator  $\sigma$ . It follows that there exists an element  $c_i \in \mathbb{F}_{q^d}(T)$  such that

$$\sigma\left(\sum_{i=1}^s \frac{b_i}{U_1^{(i)}}\right) = \sum_{i=1}^s \frac{b_i}{U_1^{(i+1)}} + c_i^p - c_i.$$

By uniqueness of partial fraction expansions, this yields that  $b_1 = b_2 = \dots = b_s$ . In order to consider the higher powers  $j = 3, \dots, \alpha$ , one may then proceed inductively, or alternatively, via a standard Witt vector construction [6].  $\square$

## 6. GALOIS MODULE STRUCTURE

Let  $\pi : X \rightarrow Y$  be a Galois ramified cover with Galois group  $H$ , and let  $df$  be a differential on  $Y$ . Let  $\pi^*$  denote the pullback. The divisor  $(\pi^*(df))_Y$  of  $\pi^*(df)$  in  $Y$  is given by  $\pi^*\text{div}_Y(df) + R_{X/Y}$ . This allows us to compute holomorphic differentials on  $X$  via functions  $g \in k(X)$  such that  $\text{div}_X(g) + \text{div}_X(df)$  is holomorphic [1].  $H$ -invariant differentials on  $X$  correspond to meromorphic differentials  $\Omega_Y(\mathcal{D})$  of  $Y$  with a well-prescribed set of poles and pole orders, where  $\mathcal{D}$  can be explicitly prescribed. We let  $\mathfrak{I}_X$  (resp.  $\mathfrak{I}_Y$ ) denote the collection of integral divisors of  $X$  (resp.  $Y$ ). Let  $df$  be a differential of  $Y$ , and let

$$R_{X/Y} = \prod_{i=1}^s \delta_i \prod_{Q_{\nu,i} \mapsto P_i} Q_{\nu,i}$$

be the ramification divisor of  $X/Y$ . An  $H$ -invariant differential on  $X$  is given by  $h df$ , where  $h \in k(Y)$ . We observe that  $h df$  is holomorphic if, and only if, the divisor  $(h)_X(\pi^*(df))_X \in \mathfrak{I}_X$ . By then taking the pushforward, we see that this condition is equivalent to

$$(h)_Y(df)_Y \cdot (\pi_*(R_{X/Y}))_Y^{\frac{1}{|H|}} \in \mathfrak{I}_Y.$$

An easy computation yields that

$$(\pi_*(R_{X/Y}))_Y = \prod_{i=1}^s (P_i)_Y^{\delta_i \frac{|H|}{e_i}},$$

where  $\delta_i$  is the differential exponent at  $P_i$ , and therefore, the set of  $H$ -invariant differentials can be identified with the space of functions

$$\begin{aligned} L_Y \left( \Omega_Y \left( \prod_{i=1}^s (P_i)_Y^{\left\lfloor \frac{\delta_i}{e_i} \right\rfloor} \right) \right) &= \left\{ f \in k(Y) : (f)_Y(df)_Y \prod_{i=1}^s (P_i)_Y^{\left\lfloor \frac{\delta_i}{e_i} \right\rfloor} \in \mathfrak{I}_Y \right\} \\ (20) \quad &= L_Y(\Omega_Y(\mathcal{D})). \end{aligned}$$

We have

$$L_Y(\Omega_Y) = \pi_*(L_X(\Omega_X \cdot R_{X/Y}^{-1})) \cong \pi_* L_X(\pi^* \text{div}_Y(dT)).$$

Here,  $X$  and  $Y$  are the curves corresponding to the function fields  $K_{q^d, P^\alpha}$  and  $\mathbb{F}_{q^d} K_{q, P^\alpha}$ , respectively. We know that

$$(21) \quad \text{div}_Y(dT) = \prod_{i=1}^s \prod_{\mathfrak{P} | P_i} \mathfrak{P}_i^S \prod_{Q | P_\infty} Q^{q-2} \cdot \text{con}_{\mathbb{F}_q(T)/\mathbb{F}_{q^d} K_{q, P^\alpha}}(\mathfrak{p}_\infty^{-2}),$$

where  $S = \alpha q^\alpha - (\alpha + 1)q^{\alpha-1}$  [12]. The divisor  $\pi^*(\text{div}_Y(dT))$  is given by

$$\pi^*(\text{div}_Y(dT)) = \mathfrak{D} \cdot \text{con}_{\mathbb{F}_{q^d} K_{q, P^\alpha}/K_{q^d, P^\alpha}}(\text{div}_Y(dT)),$$

where  $\mathfrak{D} = \mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}}$  is the different divisor

$$\mathfrak{D}_{K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}} = \left( \prod_{i=1}^s \prod_{\mathfrak{P} | \wp_i} \mathfrak{P} \right)^{\frac{q^{d(\alpha-1)}(q^d - q^s)}{q^s - 1}} \left( \prod_{\mathfrak{P} | \mathfrak{p}_\infty} \mathfrak{P} \right)^{q \left( \frac{q^{d-1} - 1}{q - 1} \right)}.$$

**Remark 6.1.** In the special case that  $s = d$ , ramification is tame in the extension  $K_{q^d, P^\alpha}/\mathbb{F}_{q^d} K_{q, P^\alpha}$ , so that  $\mathcal{D} = 0$  and the invariant elements thus satisfy  $L_X(\Omega_X)^H = L_Y(\Omega_X)$ .

A holomorphic differential on  $X$  is given by a differential of the form

$$(22) \quad \omega = \prod_{i=1}^s \prod_{k=2}^{\alpha} \lambda_{i,k}^{\mu_{i,k}} \lambda_{i,1}^{-\mu_{i,1}} dT,$$

which is invariant under the action of  $H_{q^d, M}$  [14]. By the Chinese remainder theorem, the class of an element  $D \in \mathbb{F}_{q^d}[T]$  modulo

$$P^\alpha = \prod_{i=1}^s P_i^\alpha$$

determined by the classes  $D \bmod P_i^\alpha$ . Moreover, a class  $D \bmod P_i^\alpha$  can be expressed as a  $P_i$ -adic series

$$D \bmod P_i^\alpha = a_{i,0} + a_{i,1}P_i + a_{i,2}P_i^2 + \cdots a_{i,\alpha-1}P_i^{\alpha-1} \bmod P_i^\alpha,$$

where  $a_{i,j} \in \mathbb{F}_{q^d}$  for all  $1 \leq i \leq s$  and  $0 \leq j \leq \alpha - 1$ . The action of  $D$  on  $\lambda_{i,k}$  is determined by its  $P_i$ -adic decomposition. We also have for each  $k = 1, \dots, \alpha$  that

$$(23) \quad \begin{aligned} \left( \sum_{\ell=0}^{\alpha-1} a_{i,\ell} P_i^\ell \right) *_d \lambda_{i,k} &= \left( \sum_{\ell=0}^{\alpha-1} a_{i,\ell} P_i^\ell P_i^{\alpha-k} \right) *_d \lambda_{i,\alpha} \\ &= \left( \sum_{\ell=0}^{\alpha-1} a_{i,\ell} P_i^{\alpha-k+\ell} \right) *_d \lambda_{i,\alpha} \\ &= \sum_{\ell=0}^{\alpha-1} a_{i,\ell} (P_i^{\alpha-k+\ell} *_d \lambda_{i,\alpha}) \\ &= \sum_{\ell=0}^{\alpha-1} a_{i,\ell} \lambda_{i,k-\ell}, \end{aligned}$$

where we define  $\lambda_{i,m} := 0$  whenever  $m \leq 0$ .

The action described in (23) gives rise to a representation

$$(24) \quad \begin{aligned} \rho : (\mathbb{F}_{q^d}(T)/P^\alpha)^* &\longrightarrow \mathrm{GL}(\alpha, \mathbb{F}_{q^d}) \\ \sum_{\ell=0}^{\alpha-1} a_\ell P^\ell &\mapsto \begin{pmatrix} a_0 & a_1 & \cdots & a_{\alpha-2} & a_{\alpha-1} \\ 0 & a_0 & a_1 & \cdots & a_{\alpha-2} \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_0 & a_1 \\ 0 & \cdots & \cdots & 0 & a_0 \end{pmatrix}. \end{aligned}$$

Upper triangular matrices of the form (24) are known as *Toeplitz* matrices. In this way, we obtain a representation of  $\mathbb{F}_{q^d}^*$  inside the algebraic subgroup of upper triangular matrices  $T_\alpha(\mathbb{F}_{q^d})$  given by the ideal of relations

$$I := \langle T_{i,i+\mu} - T_{j,j+\mu} \text{ for all } 1 \leq i \leq \alpha \text{ and } 0 \leq j \leq n-1 \rangle,$$

i.e., the algebraic group given by the affine coordinate ring

$$k[T_{i,j}, \det(T_{i,j})^{-1}] / \langle T_{i,j} : i > j, I \rangle$$

and the corresponding finite group of Lie type defined by the fixed points of the  $d$ -th power of the Frobenius.

**Definition.** Let  $\Delta T_\alpha$  denote the subgroup of  $T_\alpha(\mathbb{F}_{q^d})$  consisting of matrices given as in (24).

**Remark 6.2.** Let  $M \in \mathbb{F}_q[T]$  be arbitrary and nonzero. An element  $f$  is invariant under the action of  $H_{q^d, M}$  if, and only if,

$$(25) \quad \boxed{\sigma_D \circ \sigma(x) = \sigma \circ \sigma_D(x), \text{ for all } D \in \mathbb{F}_{q^d}[T]/M.}$$

We now recall a classical result of descent theory. From a cohomological point of view, there is a natural action of  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$  on the  $\mathbb{F}_{q^d}$ -vector space

$$V = H^0(K_{q^d, M}, \Omega_{K_{q^d, M}}).$$

Let us consider a basis  $\{\omega_1, \dots, \omega_g\}$  of  $V$ , where  $g$  denotes the genus of  $K_{q^d, M}$ . Define the map

$$\begin{aligned} \text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) &\rightarrow \text{GL}(V) \\ \sigma &\mapsto \rho(\sigma) : v \mapsto v^\sigma \end{aligned}$$

For each basis element  $\omega_i$ ,  $1 \leq i \leq g$  we write

$$\omega_i^\sigma = \sum_{\nu=1}^g \rho(\sigma)_{\nu, i} \omega_\nu.$$

Then, since  $(\omega_i^{\sigma_1})^{\sigma_2} = \omega_i^{\sigma_1 \sigma_2}$ , we have

$$\omega_i^{\sigma_1 \sigma_2} = \sum_{\nu, \mu=1}^g \rho(\sigma_1)_{\nu, i}^{\sigma_2} \rho(\sigma_2)_{\mu, \nu} \omega_\mu$$

so that the function  $\rho$  satisfies the cocycle condition  $\rho(\sigma_1 \sigma_2) = \rho(\sigma_1)^{\sigma_2} \rho(\sigma_2)$ . The multidimensional Hilbert's 90 theorem asserts that there is an element  $\wp \in \text{GL}(V)$  such that  $\rho(\sigma) = \wp^{-1} \sigma \wp$ . Moreover, the elements  $\omega'_i = \omega_i \wp^{-1}$  are  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -invariant since

$$(\omega_i \wp^{-1})^\sigma = (\omega_i^\sigma) (\wp^{-1})^\sigma = \omega_i \rho(\sigma) (\wp^{-1})^\sigma = \omega_i \wp^{-1} \wp^\sigma (\wp^{-1})^\sigma = \omega_i \wp^{-1}.$$

From now on  $\{\omega_i\}_{i=1, \dots, g}$  denotes an  $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ -invariant basis. An arbitrary element  $\omega \in V$  is written as

$$\omega = \sum_{i=1}^g a_i \omega_i$$

and the action of  $\sigma_D$  with respect to this basis is given by a representation

$$\begin{aligned} G_{q^d, M} &\rightarrow \text{GL}(V) \\ \sigma_D &\mapsto A(\sigma_D) =: A_D \end{aligned}$$

The condition of (25) is now expressed as the matrix condition

$$A_D \begin{pmatrix} a_1^q \\ \vdots \\ a_g^q \end{pmatrix} = A_D^q \begin{pmatrix} a_1^q \\ \vdots \\ a_g^q \end{pmatrix} \Leftrightarrow A_D^{q^{d-1}} \begin{pmatrix} a_1 \\ \vdots \\ a_g \end{pmatrix} = A_D \begin{pmatrix} a_1 \\ \vdots \\ a_g \end{pmatrix}.$$

Equivalently, the common eigenspace in  $V$  of the eigenvalue 1 of all matrices of the form  $A_D^{q^{d-1}-1}$  gives the space of  $H_{q^d, M}$ -invariant differentials. The space  $L_Y(\Omega_Y(\mathcal{D}))$  (see (20)) consists of meromorphic differentials with allowed poles at  $\mathcal{D}$ , and it is only necessary to select the holomorphic differentials among these.

We now return to the case  $M = P^\alpha$  and examine invariant rings. The group  $\Delta T_\alpha$  is clearly abelian. The action of (24) has an extension to the polynomial ring  $\mathbb{F}_{q^d}[\lambda_{i,0}, \dots, \lambda_{i,\alpha-1}]$ . Consider the vector space of polynomials of multidegree, which we denote by  $\text{mdeg}$ , bounded by  $(\mu_0, \dots, \mu_{\alpha-1})$ :

$$W_{\bar{\mu}} := \{f \in \mathbb{F}_{q^d}[\lambda_0, \dots, \lambda_{\alpha-1}] : \text{mdeg}(f) \leq (\mu_0, \dots, \mu_{\alpha-1})\} \quad (\bar{\mu} = (\mu_0, \dots, \mu_{\alpha-1})).$$

The space  $W_{\bar{\mu}}$  inherits a unique representation of the group  $(\mathbb{F}_{q^d}(T)/P^\alpha)^*$ . Therefore, we obtain

$$(26) \quad H^0(Y, \Omega_Y) \subset L_Y(\Omega_Y(\mathcal{D})) = W_{\bar{\mu}}^{H_{q^d, P^\alpha}}.$$

We thus consider the polynomial ring  $\mathbb{F}_{q^d}[\lambda_0, \dots, \lambda_{\alpha-1}]$  equipped with the natural extension of the linear action of (23) which is represented by the matrix in (24). The space of invariants  $\mathbb{F}_{q^d}[\lambda_0, \dots, \lambda_{\alpha-1}]^{H_{q^d, P^\alpha}}$  is a finitely generated ring.

Consider the subgroup  $H < \text{GL}(\alpha, \mathbb{F}_{q^d})$  which consists of unitriangular elements of the form (24), corresponding to the wild component of the cover  $X \rightarrow Y$ . Let us view the particular case of  $\text{GL}(3, \mathbb{F}_3)$ , in order to simplify the presentation. In this case, the subgroup  $H$  of Toeplitz matrices take the form

$$\sigma = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b \in \mathbb{F}_3.$$

Viewing this matrix as acting on the ring  $\mathbb{F}_3[x, y, z]$ , we find  $\sigma(x) = x$ , and

$$\sigma(y^3 - yx^2) = y^3 + a^3x^2 - yx^2 - ax^3 = y^3 + ax^2 - yx^2 - ax^3 = y^3 - yx^2.$$

By modular representation theory [2, Corollary 3.1.6], a homogeneous system of parameters  $\{f, g, h\}$  for  $\mathbb{F}_3[x, y, z]$  satisfies

$$\mathbb{F}_3[f, g, h] = \mathbb{F}_3[x, y, z]^H$$

if, and only if,

$$\deg(f) \deg(g) \deg(h) = |H|.$$

By definition,  $|H| = 9$ . Also by definition, we have

$$\sigma(y) = y + ax,$$

so any invariant involving  $y$  must have degree at least  $q$ . The same is true for  $z$  as

$$\sigma(z) = z + ay + bx.$$

As the invariant for  $x$  is already of minimal degree (one), it follows that the remaining two invariants must be of degree  $3 \mid 9$  if  $\mathbb{F}_3[x, y, z]^H$  is polynomial. Let us then examine the action of  $\sigma$  on all homogeneous terms of degree 3 in the variables  $x, y$ , and  $z$ :

Element	Constant	$x$	$x^2$	$x^3$
$x^3$	0	0	0	0
$y^3$	0	0	0	$a$
$z^3$	$ay^3$	0	0	$b$
$x^2y$	0	0	0	$a$
$xy^2$	0	0	$2ay$	$a^2$
$x^2z$	0	0	$ay$	$b$
$xz^2$	0	$a^2y^2 + 2ayz + z^2$	$2aby + 2bz$	$b^2$
$y^2z$	$ay^3 + y^2z$	$2a^2y^2 + by^2 + 2ayz$	$a^3y + 2aby + a^2z$	$a^2b$
$yz^2$	$a^2y^3 + 2ay^2z + yz^2$	$a^3y^2 + 2aby^2 + 2a^2yz + 2byz + az^2$	$2a^2by + b^2y + 2abz$	$ab^2$
$xyz$	0	$ay^2 + yz$	$a^2y + by + az$	$ab$

*The table of remainder coefficients via the  $H$ -action.*

Note that we are only considering the remainder coefficients, as the unitriangular action always returns an expansion containing the original element (the left-hand column). Clearly  $f = x$  is the first invariant. The invariant of minimal degree containing  $y$  is equal to the aforementioned  $y^3 - yx^2$ . It remains then to find the third invariant of degree 3, which must contain the variable  $z$ . Examination of the coefficients in  $x^3$ , we find that there are only two other terms with equal coefficients:  $x^2z$  and  $z^3$ . But if an invariant contains these two terms, then as  $x^2z$  has a coefficient of  $ay$  on  $x^2$ , it follows that it must contain another term with a coefficient equal to a multiple of  $ay$  on  $x^2$ . This occurs in only one element:  $xy^2$ . But the coefficient of  $x^3$  on  $xy^2$  is equal to  $a^2$ , which matches no other terms of degree 3. Thus there is no invariant of degree 3 containing the element  $z$ . This argument may be easily generalised to our case of  $\mathrm{GL}(\alpha, \mathbb{F}_{q^d})$ . We thus obtain:

**Theorem 6.3.** *Let  $H$  be the subgroup of upper unitriangular Toeplitz matrices in  $\mathrm{GL}(\alpha, \mathbb{F}_{q^d})$ . The ring of invariants  $\mathbb{F}_{q^d}[\lambda_0, \dots, \lambda_{\alpha-1}]^H$  is not polynomial.*

By Lemma 2.3, we have  $H_{q^d, P^\alpha} = (\sigma - 1)G_{q^d, P^\alpha}$ . When  $\alpha = 3$ , for example, an element of  $H_{q^d, P^\alpha}$  takes the form (up to the tame part, i.e., a diagonal multiple)

$$(27) \quad \begin{pmatrix} 1 & \sigma(a) & \sigma(b) \\ 0 & 1 & \sigma(a) \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a^q & b^q \\ 0 & 1 & a^q \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\ = \begin{pmatrix} 1 & a^q - a & a(a^q - a) + b^q - b \\ 0 & 1 & a^q - a \\ 0 & 0 & 1 \end{pmatrix}.$$

This may be easily generalised to arbitrary  $\alpha$ :

**Proposition 6.4.** *The upper diagonal entries of matrices for elements of  $H_{q^d, P^\alpha}$  are  $\mathbb{F}_{q^d}$ -multiples of Frobenius differences  $x^q - x$  ( $x \in \mathbb{F}_{q^d}$ ).*

An explicit description of the holomorphic differentials of  $K_{q, P^\alpha}$  requires computation of classical binomial coefficients occurring in the  $H_{q^d, P^\alpha}$ -action on the canonical basis consisting of elements of the form (22). Although it would be desirable, no basis of cyclotomic holomorphic differentials is currently known which allows a description of this action in terms of the function field binomial coefficients  $\begin{bmatrix} M \\ i \end{bmatrix}_{q^d}$  appearing in the expansion of the additive Carlitz action (1)

$$u_{q^d, M} = \sum a_i \tau_{q^d}^i(u) = \sum_{i=0}^{\deg(M)} \begin{bmatrix} M \\ i \end{bmatrix}_{q^d} u^{q^{di}}.$$

This fact is owed to linear dependence between terms: The Carlitz module  $\Lambda_{q^d, M}$  is too small as an  $\mathbb{F}_{q^d}$ -vector space of dimension equal  $\deg(M)$ , far from sufficient to match genus growth [12, Proposition 12.7.1]. We leave this as an open question for a future work.

## REFERENCES

- [1] H. Boseck. Zur Theorie der Weierstrasspunkte *Math. Nachr.*, 19: 29-63, 1958.
- [2] E. Campbell and D. Wehlau. *Modular Invariant Theory*. Springer, 2011.
- [3] R. Chapman. Carlitz modules and normal integral bases. *J. London Math. Soc.*, 44(2):250-260, 1991.
- [4] V.G. Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

- [5] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1998.
- [6] M. Hazewinkel. *Handbook of Algebra, Volume 6*. Elsevier, 2009.
- [7] Y. Ihara. Profinite Braid Groups, Galois Representations and Complex Multiplications. *Ann. Math.* 123, 43–106 (1986).
- [8] A. Keller. *Cyclotomic Function Fields with Many Rational Places*. Doctoral thesis, Saarbrücken, 2000.
- [9] M. Rosen. *Number Theory in Function Fields*. Graduate Texts in Mathematics. Springer New York, 2002.
- [10] J.C. Salas-Torres, M. Rzedowski-Calderón and G.D. Villa-Salvador. A combinatorial proof of the Kronecker–Weber Theorem in positive characteristic. *Finite Fields App.*, 26:144–161, 2014.
- [11] T. Sekiguchi, F. Oort, and N. Suwa. On the deformation of Artin-Schreier to Kummer. *Ann. Sci. École Norm. Sup.*, 22(3):345–375, 1989.
- [12] G.D. Villa-Salvador. *Topics in the Theory of Algebraic Function Fields*. Mathematics: Theory & Applications. Birkhäuser Boston, 2007.
- [13] Serre, J.-P. Local Fields, Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. viii+241 pp. ISBN: 0-387-90424-7
- [14] K. Ward. Explicit Galois representations of automorphisms on holomorphic differentials in characteristic  $p$ . *Finite Fields App.*, 44:34–55, 2017.